WHAT IS CLAIMED IS:

1. A method of providing high-security protection for an electronic informational resource, the program having a protected portion, the method comprising:

encrypting high-security authorization information using a first fingerprint as a key to generate an encrypted high-security authorization information, the first fingerprint being computed based on the protected portion of the program; and

upon a request to access the protected portion of the program, decrypting the encrypted high-security authorization information using a second fingerprint, the second fingerprint being computed based on the protected portion of the program.

2. The method according to claim 1, wherein the first fingerprint and second fingerprint are one-way hashes computed from a portion of a memory where the protected portion of the secure program resides.

3. The method according to claim 1, further comprising:

authorizing a secure channel between the protected portion of the program and a data processing mechanism if and only if the decrypting is successful.

4. A method of establishing high-security protection for a data source using a program having a protected portion, the method comprising:

receiving high-security authorization information that is used to establish protection for the data source;

computing a fingerprint based on the protected portion of the program; and

encrypting high-security authorization information using the fingerprint.

5. The method according to claim 4, wherein the program is activated and the fingerprint is a message digest computed based on a portion of a memory where the protected portion of the activated program resides.

6. The method according to claim 4, wherein said high-security authorization information includes a password.

7. The method according to claim 4, wherein said high-security authorization information includes a token.

8. A method for high-security protection of a data source via a program, the program having a protected portion, the method comprising:

upon activating the program, computing a fingerprint based on the protected portion of the program; and

verifying that the protected portion of the program is not tampered through decrypting an encrypted high-security authorization information using the fingerprint.

9. The method according to claim 8, further comprising:

prior to activating the program, receiving low-security authorization information;

authenticating the low-security authorization information,

if said low-security authorization information is authenticated, allowing the activating of the program; and

if said low-security authorization information is not authenticated, not activating the program.

10. The method according to claim 8, further comprising:

if the protected portion of the program is not tampered, authorizing a secure channel between the protected portion of the secure program and a data processing mechanism, the data processing mechanism accessing information from the data source through the secure channel.

11. A method for secure data replication, comprising:

activating a protected portion of a program, said protected portion replicating data stored in a first database in a second database;

establishing a first secure session, between the protected portion and the first database to copy data from the first database, using a first fingerprint computed based on the protected portion; and

establishing a second secure session, between the protected portion and the second database to replicate the data in the second database, using a secondfingerprint computed based on the protected portion.

12. The method according to claim 11, wherein the first fingerprint is a first message digest and establishing a first secure session comprises:

computing the first fingerprint from the protected portion of the program;

decrypting an encrypted authorization information using thefirst fingerprint as a key; and

if the encrypted authorization information is successfully decrypted, copying the data from the first database.

13. The method according to claim 11, wherein the second fingerprint is a second message digest and establishing a second secure session comprises:

computing the second message digest from the protected portion of the program;

decrypting an encrypted authorization information using the second fingerprint as a key; and

if the encrypted authorization information is successfully decrypted, , duplicating the data in the second database.

14. A system, comprising:

a program having a protected portion;

a high-security set up mechanism for establishing high-security protection to a data resource using the protected portion of the program based on encrypted high-security authorization information generated using a fingerprint computed based on the protected portion of the program; and

a high-security protection mechanism for enforcing high-security protection on the protected portion of the program using the encrypted high-security authorization information.

15. The system according to claim 14, wherein the protected portion includes an encryption function that computes the fingerprint based on the protected portion of the program.

16. The system according to claim 14, wherein the high-security set up mechanism comprises:

an encryption mechanism for encrypting a high-security authorization information to generate, using the fingerprint as a key, the encrypted high-security authorization information; and

an encrypted high-security authorization information storage for storing the encrypted high-security authorization information.

17. The system according to claim 16, wherein the high-security protection mechanism comprises:

a high-security information retrieval mechanism for accessing encrypted high-security authorization information from the encrypted high-security authorization information storage; and

a decryption mechanism for decrypting, using another fingerprint as a key, the encrypted high-security authorization information, another fingerprint being computed based on the protected portion of the program.

18. A computer program product including computer program code to cause a microprocessor to perform a method of providing high-security protection for a data resource , the program having a protected portion, the method comprising:

encrypting high-security authorization information using a first fingerprint to generate an encrypted high-security authorization information, the first fingerprint being computed based on the protected portion of the program; and

upon a request to access the protected portion of the program, decrypting the encrypted high-security authorization information using a second fingerprint, the second fingerprint being computed based on the protected portion of the program.

19. The computer program product according to claim 18, wherein the first fingerprint and second fingerprint are one-way hashes computed from a portion of a memory where the protected portion of the secure program resides.

20. The computer program product according to claim 18, the method further comprising:

authorizing a secure channel between the protected portion of the program and a data processing mechanism if the decrypting is successful, the data processing mechanism accessing the protected portion of the program through the secure channel.

21. A computer program product including computer program code to cause a microprocessor to perform a method of establishing high-security protection for a data resource, the program having a protected portion, the method comprising:

receiving high-security authorization information used to establish protection for the data resource;

computing a fingerprint based on a protected portion of the program; and

generating encrypted high-security authorization information using the fingerprint.

22. The computer program product according to claim 21, wherein the program is activated and the fingerprint is a message digest computed based on a portion of a memory where the protected portion of the activated program resides.

23. The computer program product according to claim 21, wherein said high-security authorization information includes a password.

24. A computer program product including computer program code to cause a microprocessor to perform a method for high-security protection of a data resource via a program, the program having a protected portion, the method comprising:

upon activating the program, computing a fingerprint based on the protected portion of the program; and

verifying that the protected portion of the program is not tampered through decrypting an encrypted high-security authorization information using the fingerprint.

25. The computer program product according to claim 25, further comprising:

prior to activating the program, receiving low-security authorization information;

authenticating the low-security authorization information;

if said low-security authorization information is authenticated, allowing the activating of the program; and

if said low-security authorization information is not authenticated, not activating the program, computing a fingerprint and verifying that the protected portion of the program is tampered.

26. The computer program product according to claim 24, further comprising:

if the protected portion of the program is not tampered, authorizing a secure channel between the protected portion of the secure program and a data processing mechanism, the data processing mechanism accessing information from the data resource through the secure channel.

27. A computer program product including computer program code to cause a microprocessor to perform a method for secure data replication, the method comprising:

activating a protected portion of a program, said protected portion replicating data stored in a first database in a second database;

establishing a first secure session, between the protected portion and the first database to copy data from the first database, using a first fingerprint computed based on the protected portion; and

establishing a second secure session, between the protected portion and the second database to replicate the data in the second database, using a second fingerprint computed based on the protected portion.

28. The computer program product according to claim 27, wherein the first fingerprint is a first message digest and establishing a first secure session comprises:

computing the first fingerprint from the protected portion of the program;

decrypting an encrypted authorization information using the first fingerprint as a key; and

if the encrypted authorization information is successfully decrypted, copying the data from the first database.

29. The computer program product according to claim 27, wherein the second fingerprint is a second message digest and establishing a second secure session composes:

computing the second fingerprint from the protected portion of the program;

decrypting an encrypted authorization information using the second fingerprint as a key; and

if the encrypted authorization information is successfully decrypted, duplicating the data in the second database.